DETAILED ACTION

Information Disclosure Statement

1. The examiner has considered the information disclosure statements (IDSs) submitted on 6 December 2010, 1 February 2011, and 21 March 2011.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-5 and 7 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The random number encrypted by a second public key of another IC in the apparatus is not found in the specification. The portion pointed to by applicant uses one public key of the IC of the apparatus and no other public keys.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-5 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 1 recites the limitation "whereby a public key KT of the apparatus is used to decrypt an encrypted random number appended to the data, the random number being encrypted by the public key KT of another integrated circuit of the apparatus". It is unclear how this reads on asymmetric cryptography, as the claim states, if the same key is used to encrypt and decrypt the random number. It is also unclear how a public key is used to decrypt a number encrypted with a public key. A private key is used to decrypt items encrypted by public key.

7. Claim 1 further recites the limitation "the public key KT of another integrated circuit". There is insufficient antecedent basis for this limitation in the claim. It is unclear if this refers to the same KT disclosed above, or is claiming a new public key of another IC.

8. The issues outlined above in reference to claim 1 also apply to claim 7.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-3 and 7, as best understood, are rejected under 35 U.S.C. 102(e) as being anticipated by Auerbach et al., USPN 5,673,316.

With regard to claims 1 and 7, Auerbach discloses an integrated circuit for the authentication of a consumable storage device (secure cryptographic envelope) by an apparatus (column 1 lines 39-44), the integrated circuit including a memory space which contains encrypted data defined by a MAC applied to data (column 4 lines 25-35) relating to a consumable stored by the device (column 4 lines 9-18), the MAC being constructed of an asymmetric cryptographic function whereby a public key of the apparatus is used to decrypt an encrypted random number (random PEK, column 5 lines 63-64) appended to the data (column 6 lines 1-5) the random number being encrypted by the public key of another integrated circuit of the apparatus (column 6 lines 1-5) and a secret key of the apparatus is used to decrypt encrypted data stored in the memory space (column 10 lines 50-64).

With regard to claim 2, Auerbach discloses the circuit of claim 1 as outlined above, and further discloses the function is a hash function (column 5 lines 19-35).

With regard to claim 3, Auerbach discloses the circuit of claim 2 as outlined above, and further discloses the hash function is MD5 (column 5 lines 19-20).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 4 and 5, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over Auerbach in view of examiner’s official notice.

With regard to claims 4, Auerbach discloses the circuit of claim 2 as outlined above, and mentions using secure hash algorithms, but does not specify SHA-1 (column 5 lines 29-31). The examiner takes official notice that SHA-1 is a well known secure hash function. It would have been obvious for one of ordinary skill in the art to use SHA-1 as the “other secure hash” of Auerbach for the motivation of increased security.

With regard to claim 5, Auerbach in view of examiner’s official notice discloses the circuit of claim 4 as outlined above, and further discloses using temporary registers and rotating counters (column 6 lines 20-27).

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JACOB LIPMAN whose telephone number is (571)272-3837. The examiner can normally be reached on M-Fr.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jacob Lipman/
Primary Examiner, Art Unit 2434